Task Force Web

SSO Update
13 November 2002

LT Rajeev Parekh, TFW IA Technical Team Liaison

Outline

- Why is SSO important?
- Fleet SSO Requirements
- Laboratory Testing
- Enterprise Standards
- SAML Discussion and Summary
- Fleet SSO TRBG Install
- SSO Demo
- Developer Impacts

Single Sign On (SSO)

- **Single Sign On (SSO)** is an authentication process in a client/server relationship where the user, or client, can identify and authenticate only once and have access to more than one application, or access to a number of resources within an enterprise
  - SSO removes the need for the user to re-authenticate when switching from one application, or resource, to another

Why is SSO Important?

- Security Administration Management
- Identification and Authorization
- Access Control
- Data Integrity/ Confidentiality/ Encryption

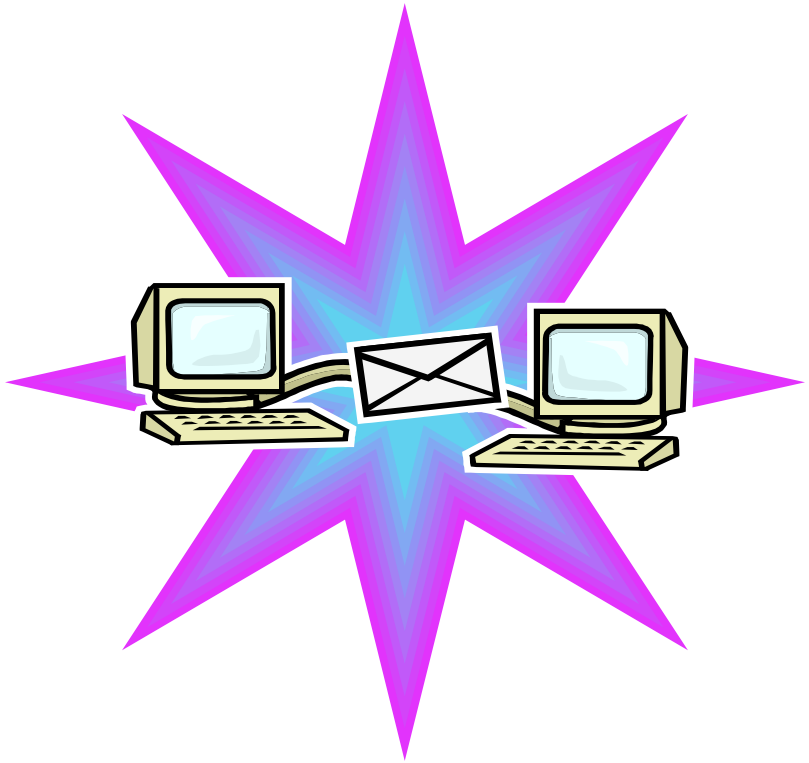
Fleet SSO Requirements

- Fleet requirements comprise four major areas
  - Security
  - Deployability
  - Admin Functionality & Supportability
  - End-to-End SSO Interoperability

Laboratory Testing

- Laboratory testing was conducted by SSC-SD on NIPRNET and SIPRNET apps hosted within the NMCI enclave for the purpose of understanding interoperability issues associated with SSO

- Results were concluded on 28 June 2002



Security Assertion Markup Language (SAML) 1.0

- **SAML** is defined as an open source, XML-based, framework for ensuring that transmitted communications are secure
  - **SAML** defines mechanisms to exchange authentication, authorization and non-repudiation information, allowing single sign-on capabilities for web services
- Basically, **SAML** is a normative specification that enables the exchange of authentication and authorization information between sites that have separate user directories and authorization policies in a coherent/uniform manner

SAML 1.0

- SAML 1.0 specification was “solidified” in April ‘02
  - Future SAML specifications will depend largely on implementation and integration requirements and deficiencies noted in the 1.0 specification
  - This 1.0 specification is the first concerted effort by the entire IT industry to secure web services architectures
- SAML 1.0 specification balloting took place in September 2002 to formalize the specification
  - There are several SAML products available (e.g., Baltimore (SelectAccess), Entegrity (AssureAccess)) with others to be provided soon (e.g., Oblix, Tivoli, et al)

SAML 1.0 Product Availability

- SAML 1.0 products are not available in significant quantities across the IT spectrum
  - There are some pre-SAML products, some of which are undergoing minor mods since the balloting to establish the 1.0 specification
  - More products can be expected to enter the open source arena now that the 1.0 specification has been firmly established
  - All current and planned SAML 1.0-based SSO products are designed for behind-the-firewall use only (out of the box configuration)
    - Baltimore and Oblix allow for the port to be changed (e.g., port 443) to operate anywhere in the enterprise

Single Sign On Security Issues

- Sun Microsystems has produced a test kit to check SAML based products for 1.0 compliance
  - In practice, the currently available Web-based SSO products are capable of providing only a Reduced Sign-On (RSO) capability since current products do not perform the initial login to the operating system
- Common Criteria Protection Profiles do not exist yet for SSO, but are under way
  - No firm date on when a PP will be produced
  - Baltimore Technologies' SelectAccess product is reported to be undergoing a PP eval, but only under the Australian equivalence

SSO Summary

- A commercial standards based E2EMD Navy enterprise SSO solution does not exist today.
- Significant issues remain for an E2E SSO solution.
  - Retention of user Authentication and Authorization across multiple AD forests/identity domains.
  - Proven capability based on OASIS SAML 1.0 interoperability standard.

Fleet SSO TRBG Install

- TFW is not ready to endorse SSO products or select an enterprise SSO solution at this time.
- The Fleet has volunteered to test an SSO solution within a single security domain (not an end-to-end solution).
  - A pre-SAML implementation based on XML has been selected for this initial test – using Oblix Netpoint 6.0
  - The objective is it will provide a good understanding of the Navy's enterprise environment upon which to base an end-to-end SSO implementation.

NESSO

- Navy Enterprise Single Sign-On (NESSO)
- Proposal submitted by FNMOC
- Funded by SPAWAR PMW-161
- Based on SAML Architecture
- Projected IOC 6 March 2003

The Bottom Line

- TFW will continue to monitor SAML developments including the NESSO program
- Oblix Netpoint 6.0 is being installed on the TRBG and the CFFC Instantiation
- This SSO solution will be tested over the next 6-9 months

TASK FORCE WEB

SSO Case Study

Application SSO Integration

- IRRI application, OPREP, selected as SSO candidate
- OPREP already successfully integrated into the Portal through the Portal Connector
- SSO Integration performed following *SSO Basics Guide* document

SSO Basics Guidance

- Three basic requirements for an application to integrate with SSO:
  - Modify the application to authorize users based on the SSO-authenticated Common Identity User ID passed in the HTTP header
  - Replace or map the application's legacy user IDs to the Common Identity User IDs
  - Install an SSO web server plug-in

OPREP SSO Modifications

- Added a new field to the existing internal user database: SSOID
- Coding Changes
  - Read Common Identity User ID from the HTTP header
  - Compare Common Identity User ID to SSOID database field
  - Grant permissions to the SSO user equivalent to logging on as the legacy application User ID

User Mapping Processes

- OPREP chose a manual mapping process
  - OPREP Administrators must assign a user's SSOID before SSO authentication will operate
- Potential automatic mapping solution
  - Users that authenticate twice in one session (once using Common Identity User ID, and the other using legacy user ID) can be automatically mapped in the internal user database
  - Further logons using Common Identity User ID will result in SSO authetication

IRRI OPREP SSO Demonstration

Actors

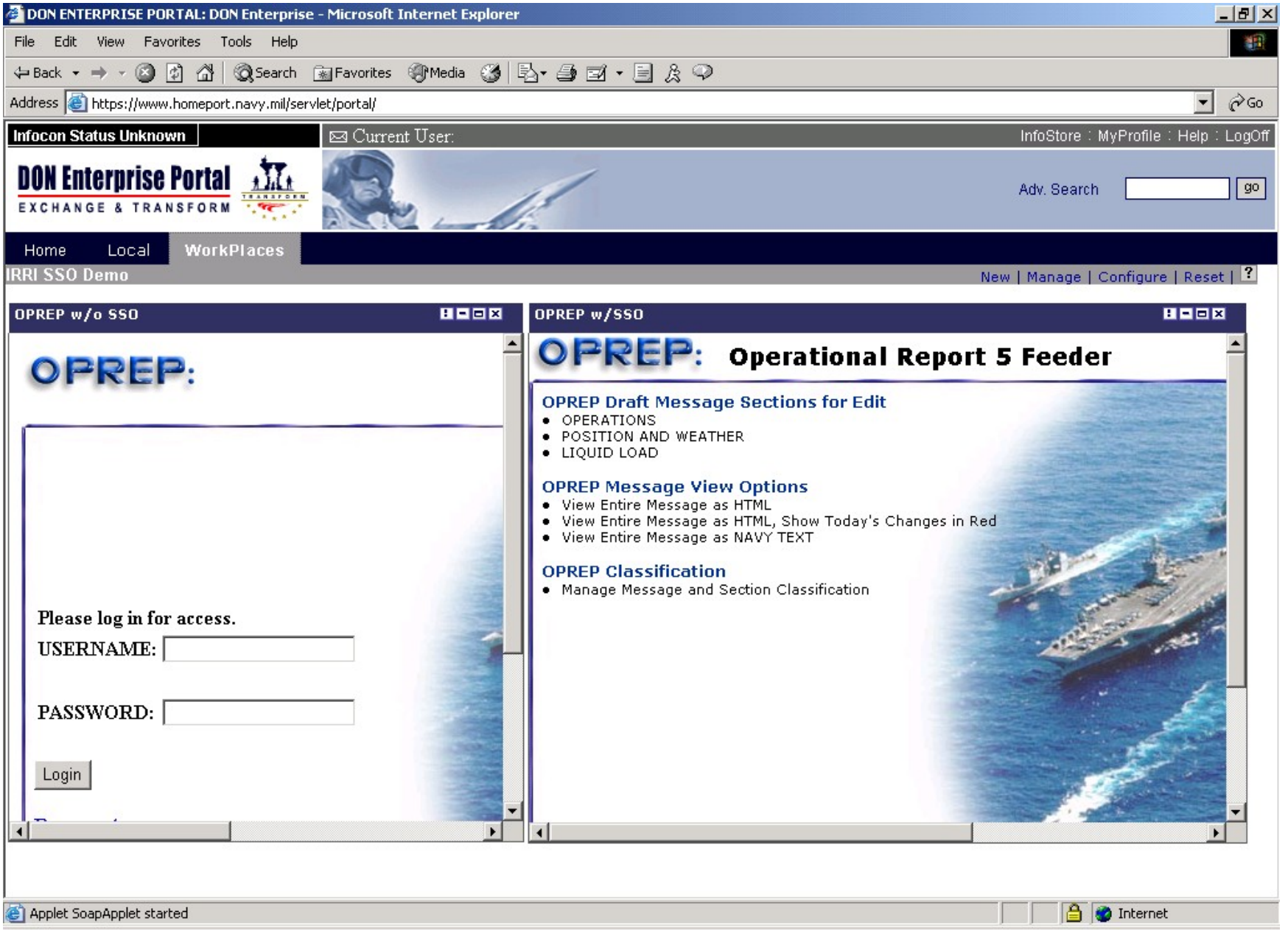
Common Identity User ID	IRRI Legacy User ID	Role/Situation
irri.user	irri.user	IRRI User (no administrative rights)
irri.admin	admin	IRRI Administrator (full administrative rights)
irri.newuser	joe_user	A new Portal User. The IRRI administrator has not yet mapped the user's legacy user ID to the new Common Identity User ID

Demo Environment

- Two versions of the IRRI OPREP application will be demonstrated
  - One integrated with the SSO
  - One without SSO integration
- Each Portal User has had an “IRRI SSO Demo” Workplace created displaying both SSO-enabled and non-SSO versions simultaneously
- The Workplace would normally have to be configured by each user separately

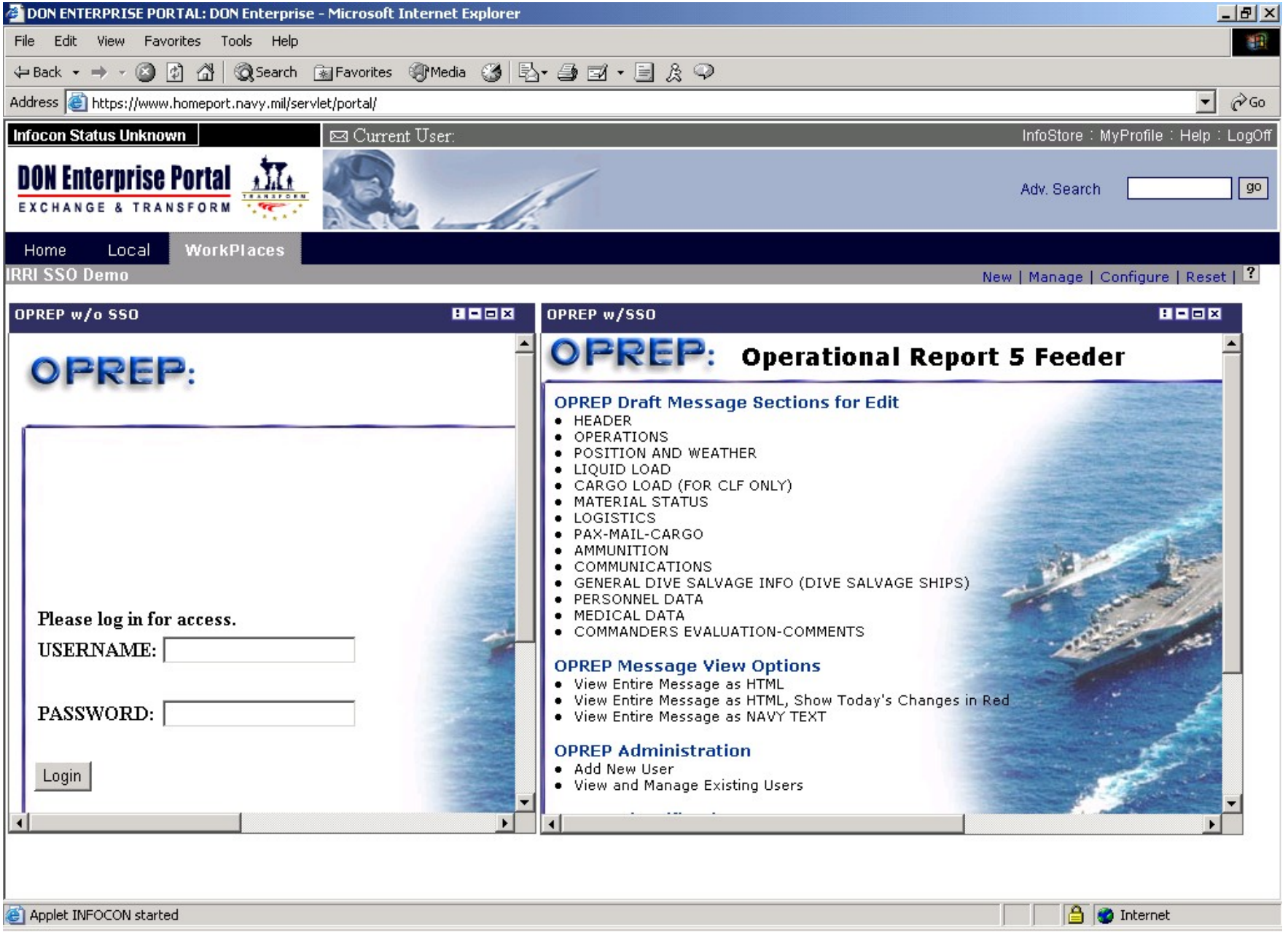
Scenario 1: Successful IRRI.User Logon

- Process:
  - Logon to the Portal using the irri.user Common Identity
  - Click on Workplaces
- What the Audience Sees:
  - Left iFrame (non-SSO) contains OPREP authentication HTML form
  - Right iFrame (SSO) contains OPREP control panel with appropriate user rights displayed for the irri.user identity
- What it Means:
  - The left iFrame is what the user would see without SSO
  - The right iFrame is what the user sees with SSO
    - No authentication necessary
    - User immediately can go about his/her business with the appropriate rights assigned to his/her legacy user account


DON ENTERPRISE PORTAL: DON Enterprise - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://www.homeport.navy.mil/servlet/portal/
Go
Infocon Status Unknown
Current User:
InfoStore : MyProfile : Help : LogOff
DON Enterprise Portal
EXCHANGE & TRANSFORM
Adv. Search
go
Home Local WorkPlaces
IRRI SSO Demo
New | Manage | Configure | Reset |
OPREP w/o SSO
OPREP:
Please log in for access.
USERNAME:
PASSWORD:
Login
OPREP w/SSO
OPREP: Operational Report 5 Feeder
OPREP Draft Message Sections for Edit
OPERATIONS
POSITION AND WEATHER
LIQUID LOAD
OPREP Message View Options
View Entire Message as HTML
View Entire Message as HTML, Show Today's Changes in Red
View Entire Message as NAVY TEXT
OPREP Classification
Manage Message and Section Classification
Applet SoapApplet started
Internet

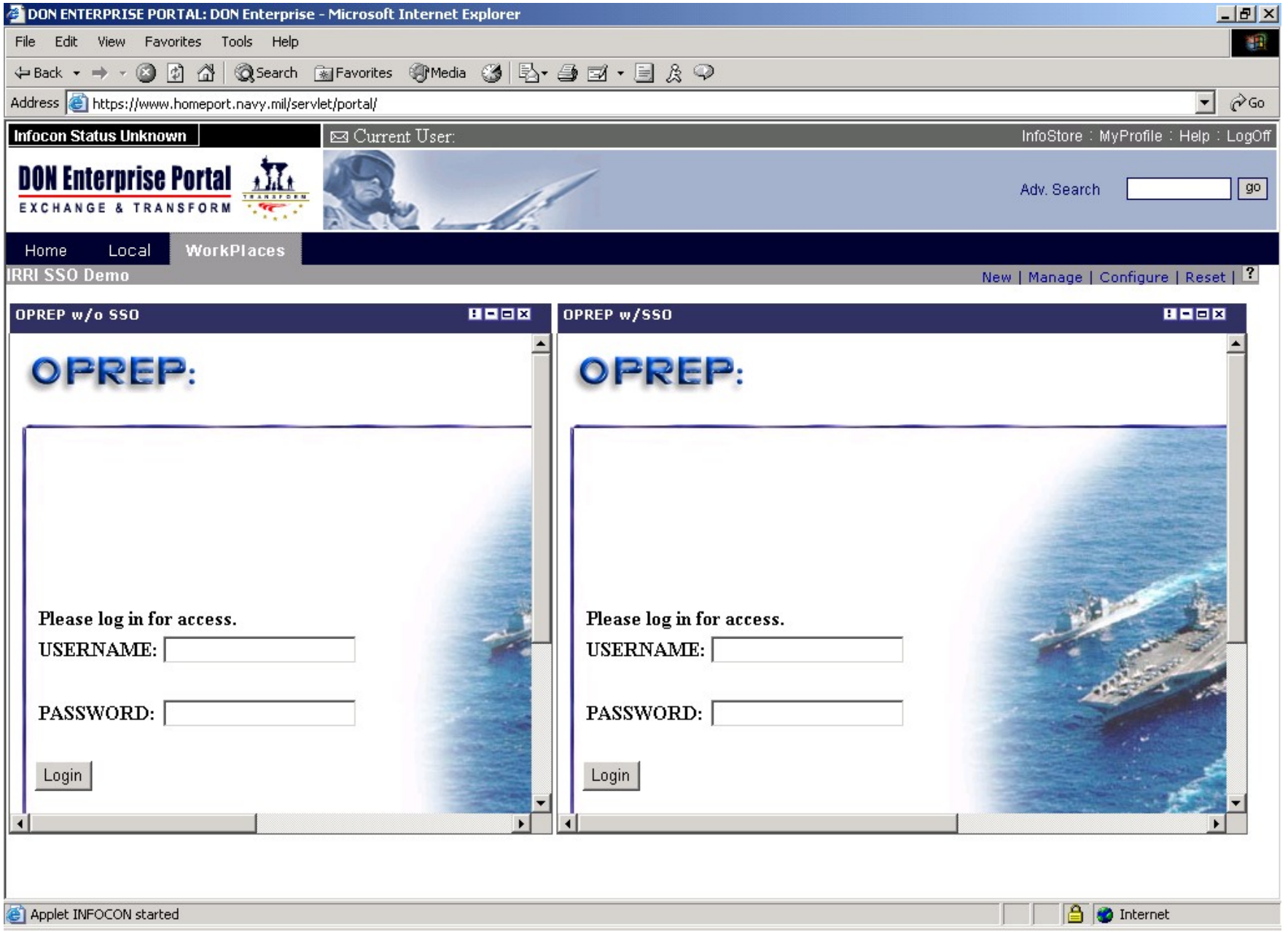
Scenario 2: Successful IRRI.Admin Logon

- Process:
  - Logon to the Portal using the irri.admin Common Identity
  - Click on Workplaces
- What the Audience Sees:
  - Left iFrame (non-SSO) contains OPREP authentication HTML form
  - Right iFrame (SSO) contains OPREP control panel with appropriate user rights displayed for the irri.admin identity
- What it Means:
  - The left iFrame is what the user would see without SSO
  - The right iFrame is what the user sees with SSO
    - No authentication necessary
    - Administrator immediately can go about his/her business with the appropriate rights assigned to his/her legacy admin account
    - The control panel is populated with additional information/controls based on the additional rights permitted for the administrator


DON ENTERPRISE PORTAL: DON Enterprise - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://www.homeport.navy.mil/servlet/portal/
Go
Infocon Status Unknown
Current User:
InfoStore : MyProfile : Help : LogOff
DON Enterprise Portal
EXCHANGE & TRANSFORM
Adv. Search
go
Home
Local
WorkPlaces
IRRI SSO Demo
New | Manage | Configure | Reset |
OPREP w/o SSO
OPREP:
Please log in for access.
USERNAME:
PASSWORD:
Login
OPREP w/SSO
OPREP: Operational Report 5 Feeder
OPREP Draft Message Sections for Edit
HEADER
OPERATIONS
POSITION AND WEATHER
LIQUID LOAD
CARGO LOAD (FOR CLF ONLY)
MATERIAL STATUS
LOGISTICS
PAX-MAIL-CARGO
AMMUNITION
COMMUNICATIONS
GENERAL DIVE SALVAGE INFO (DIVE SALVAGE SHIPS)
PERSONNEL DATA
MEDICAL DATA
COMMANDERS EVALUATION-COMMENTS
OPREP Message View Options
View Entire Message as HTML
View Entire Message as HTML, Show Today's Changes in Red
View Entire Message as NAVY TEXT
OPREP Administration
Add New User
View and Manage Existing Users
Applet INFOCON started
Internet

Scenario 3: IRRI.NewUser Logon

- Process:
  - Logon to the Portal using the irri.newuser Common Identity
  - Click on Workplaces
  - Logon to OPREP (right hand iFrame) using legacy User ID and password
- What the Audience Sees:
  - Left iFrame (non-SSO) contains OPREP authentication HTML form
  - Right iFrame (SSO) contains OPREP authentication HTML form
- What it Means:
  - The left iFrame is what the user would see without SSO
  - The right iFrame is what the user sees with SSO
    - This user has not yet been configured by the IRRI Administrator to use SSO authentication
    - The user may still authenticate using their legacy user ID and password – no loss of capability due to the SSO process being incomplete


DON ENTERPRISE PORTAL: DON Enterprise - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://www.homeport.navy.mil/servlet/portal/
Go
Infocon Status Unknown
Current User:
InfoStore : MyProfile : Help : LogOff
DON Enterprise Portal
EXCHANGE & TRANSFORM
Adv. Search
go
Home
Local
WorkPlaces
IRRI SSO Demo
New | Manage | Configure | Reset |
OPREP w/o SSO
OPREP:
Please log in for access.
USERNAME:
PASSWORD:
Login
OPREP w/SSO
OPREP:
Please log in for access.
USERNAME:
PASSWORD:
Login
Applet INFOCON started
Internet

Scenario 4: IRRI.NewUser SSO Config.

- Process:
  - Logon to the Portal using the irri.admin Common Identity
  - Modify joe_user in the OPREP application to assign the proper SSO User ID (irri.newuser)
  - Logout of Portal (close browser window)
  - Logon to the Portal using the irri,newuser Common Identity
- What the Audience Sees:
  - IRRI Admin uses the service through the Portal interface to manage users
  - When irri.newuser authenticates to the Portal this time, there is no prompt for re-authentication by OPREP
- What it Means:
  - An interactive display of how an administrator might have to migrate a new Portal user from the legacy system to the SSO
  - Other applications may choose to automatically map legacy user IDs to Common Identity User IDs programmatically, as described in the SSO Basics Guide

What does this mean to you as a Developer?

- A pre-SAML SSO product is being explored for the 2BG rollout (Oblix Netpoint 6.0)
- NESSO is also being developed for long-term SAML compliance
- An SSO PP is being written for TFW
- You should be aware that future apps that are web-enabled will need an SSO plug-in.
- Include SSO/SAML in your coding strategy!

Questions?

LT Rajeev Parekh
rajeev.parekh@navy.mil